НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Інститут телекомунікаційних систем

Кафедра Телекомунікаційних систем

«До захисту допущено»
Завідувач кафедри
_____ Леонід УРИВСЬКИЙ
«___»_____20__ р.

Дипломна робота
на здобуття ступеня бакалавра
зі спеціальності 172 Телекомунікації та радіотехніка
на тему: «Методи забезпечення інформаційної безпеки в системах управління ТКМ»

Виконала:
студентка IV курсу, групи ТС-61
Христина АТАМАНЧУК _____

Керівник:
Старший викладач кафедри ТС
Олександр ВАКУЛЕНКО _____

Рецензент:
Кандидат наук, доцент кафедри телекомунікацій ІТС
Валерій ЯВІСЯ _____

Засвідчую, що у цій дипломній роботі немає запозичень з праць інших авторів без відповідних посилань.
Студент (-ка) _____

Київ – 2020 року

Національний технічний університет України

«Київський політехнічний інститут імені Ігоря Сікорського»

Інститут телекомунікаційних систем

Кафедра Телекомунікаційних систем

Рівень вищої освіти – перший (бакалаврський)

Спеціальність – 172 Телекомунікації та радіотехніка

Програма професійного спрямування (спеціалізація) – «Телекомунікаційні системи та мережі»

ЗАТВЕРДЖУЮ

Завідувач кафедри

_____ Леонід УРИВСЬКИЙ

«___»_____20__ р.

ЗАВДАННЯ

на дипломну роботу студенту

Атаманчук Христина Володимирівна

1. Тема роботи «Методи забезпечення інформаційної безпеки в системах управління ТКМ», керівник роботи Вакуленко Олександр Володимирович старший викладач кафедри ТС, затверджені наказом по університету від 30 березня 2020 р. № 924-с

2. Термін подання студентом роботи 12 червня 2020 р.

3. Вихідні дані до роботи – джерела інформаційної безпеки, системи DLP,загрози інформаційної безпеки

4. Зміст роботи: аналіз сучасного стану інформаційної безпеки в системах управління ТКМ; аналіз інформаційної безпеки; сучасний стан інформаційної безпеки в Україні; принципи забезпечення інформаційної безпеки; інформаційна безпека; структура інформаційної-телекомунікаційної системи типового підприємства; поняття загрози інформаційної безпеки підприємства; джерела загроз; класифікація загроз інформаційним ресурсам підприємства; забезпечення інформаційної безпеки в системах управління ТКМ; інформаційна безпека в системах управління ТКМ; управління інцидентами інформаційної безпеки в системах управління ТКМ.

5. Перелік ілюстративного матеріалу (із зазначенням плакатів, презентацій тощо) :

1) Тема, мета та завдання бакалаврської роботи;
2) Основні функції DLP-систем;
3) Створення системи захисту;
4) Принцип роботи DLP;
5) Тема, мета та завдання бакалаврської роботи;
6) Функціональна схема шлюзового DLP-рішення;
7) Функціональна схема хостового DLP рішення.

6. Дата видачі завдання _____

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів роботи	Примітка
1.	Аналіз сучасного стану інформаційної безпеки в системах уплавління ТКМ	13.04.2020 – 19.04.2020	Виконала
2.	Принципи забезпечення інформаційної безпеки	20.04.2020 – 26.04.2020	Виконала
3.	Забезпечення інформаційної безпеки в системах управління ТКМ	27.04.2020 – 03.05.2020	Виконала
4.	Написання висновків до розділів і усього диплому	04.05.2020 – 10.05.2020	Виконала
5.	Кінцеве оформлення роботи (нумерація сторінок, рисунків, розміщення розташування тексту та розділових знаків тощо), переліку умовних позначень, скорочень і літератури	11.05.2020 – 17.05.2020	Виконала

Студент Христина АТАМАНЧУК

Керівник роботи Олександр ВАКУЛЕНКО

РЕФЕРАТ

Текстова частина дипломної роботи: 55 с., 8 рис., 13 джерел.

В даній роботі розглядається поняття інформаційної безпеки телекомунікаційної мережі та підприємства, сучасний стан інформаційної безпеки України, поняття загроз інформаційної безпеки підприємства та ТКМ, також наведено класифікацію загроз інформаційним ресурсам підприємства.

Описано поняття DLP-систем та як їх використовувати в сучасному підприємстві, наведено класифікацію DLP-систем та представлено їх принцип роботи.

ІНФОРМАЦІЙНА БЕЗПЕКА, DLP-СИСТЕМИ, ІНФОРМАЦІЙНА БЕЗПЕКА ТЕЛЕКОМУНІКАЦІЙНОЇ МЕРЕЖІ, ЗАГРОЗИ, СИСТЕМИ УПРАВЛІННЯ ТКМ.

ABSTRACT

Text part of the thesis: 55 pages, 8 figures, 13 sources.

This paper considers the concept of information security of telecommunications network and enterprise, the current state of information security of Ukraine, the concept of threats to information security of enterprises and TCM, as well as the classification of threats to information resources of the enterprise.

The concept of DLP-systems and how to use them in a modern enterprise is described, the classification of DLP-systems is given and their principle of operation is presented.

INFORMATION SECURITY, DLP-SYSTEMS, INFORMATION SECURITY OF TELECOMMUNICATIONS NETWORK, THREATS, TKM MANAGEMENT SYSTEMS.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

CD	Compact Disc
DDoS	(Distributed) Denial-of-service attack
DLP	Data Leak Prevention
DVD	Digital Versatile Disc
FTP	File Transfer Protocol
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
IP	Internet Protocol
ISO	Infrared Space Observatory
IT	Інформаційні технології
ЗМІ	Засоби масової інформації
ІБ	Інформаційна безпека
ІС	Інформаційна система
ІТС	Інформаційно-телекомунікаційна система
НСД	Несанкціонований доступ
ОС	Обчислювальна система
СНД	Співдружність Незалежних Держав
СУБД	Система управління базами данних
ТКМ	Телекомунікаційна кабельна мережа

ВСТУП

Нашу добу не даремно називають інформаційною. І справа тут не тільки в тому, що значна частка національного багатства сучасних країн створюється в сфері інформаційних технологій. Сучасна людина для успішної життєдіяльності не може бути осторонь інформаційних потоків. Але головна складність нині не в тому, щоб отримати певну інформацію, а в тому, щоб визначити, яка інформація потрібна і як її зберегти.

Однією з найактуальніших проблем сучасного суспільства є потреба в інформаційному забезпеченні всіх сфер діяльності людини та надійному захисті цієї інформації. Забезпечення потрібного рівня інформаційної безпеки досягається за допомогою застосування різноманітних засобів та заходів, зокрема, створення комплексної системи захисту інформації.

« Проблема витоку інформації є дуже актуальною. Великий відсоток витоку здійснюється шляхом порушення політики безпеки, несанкціонованого доступу, навмисного та випадкового. Високий рівень інформаційної безпеки підприємства досягається шляхом розробки ефективної політики безпеки і, як наслідок, оптимальних правил розмежування доступу. Засоби, що реалізують політику безпеки, здійснюють контроль над взаємодією користувачів та інформаційних ресурсів, є ключовою частиною підсистеми керування доступом. Підвищення ефективності роботи цих засобів є важливим завданням.» [13]

Поширені засоби захисту інформації (Gartner стверджує, що кожна третя у світі компанія вже використовують DLP) знімає тільки одну частину проблеми - випадкові витоки, і ніяк не впливають на зловмисні. Питання тут швидше в сприйнятті DLP-систем як програмного забезпечення, здатного самостійно, без зусиль з боку служб безпеки інформації, боротися з витоками, що є суттєвою помилкою. І якщо з випадковими витоками DLP дійсно справляється, то боротьба зі зловмисними вимагає серйозної

консалтингової складової в DLP-проектах на етапі підготовки впровадження та супроводу системи, розслідувань інцидентів.

Розпізнавання конфіденційної інформації в DLP-системах здійснюється двома способами: аналізом формальних ознак та контенту. Перший спосіб дозволяє уникнути помилкових спрацьовувань, але вимагає попередньої класифікації документів, впровадження міток, збору сигнатур і т.д. Пропуски конфіденційної інформації (помилки другого роду) при цьому методі цілком вірогідні, якщо конфіденційний документ не піддався попередній класифікації. Другий спосіб дає помилкові спрацьовування, зате дозволяє виявити пересилання конфіденційної інформації не тільки серед документів з грифом, але й без нього. У хороших DLP-системах, для безпеки компанії, об'єднуються два способи обробки інформації.

Через тенденцію витоку інформації, використання методів та моделей управління інформаційною безпекою в інформаційно-телекомунікаційних системах підприємства з використанням DLP-систем є актуальним питанням.

Мета – провести аналіз сучасного стану інформаційної безпеки в системах управління ТКМ та розглянути принципи забезпечення інформаційної безпеки, а також забезпечення інформаційної безпеки в системах управління телекомунікаційних мереж.

1 АНАЛІЗ СУЧАСНОГО СТАНУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В СИСТЕМАХ УПРАВЛІННЯ ТКМ

1.1 Аналіз інформаційної безпеки

«Діяльність із забезпечення інформаційної безпеки здійснюється за допомогою різних способів, засобів та прийомів, які в правильному поєднанні складають метод. Метод забезпечення інформаційної безпеки передбачає певну послідовність дій на підставі конкретного плану. Методи можуть значно змінюватися і варіюватися в залежності від типу діяльності, в якій вони використовуються, а також сфери застосування» [1].

Важливими методами аналізу стану інформаційної безпеки є методи опису та класифікації.

Для здійснення ефективного захисту інформаційного середовища ТКМ, потрібно спершу описати, а лише потім класифікувати різні види загроз та небезпек, ризиків та викликів і відповідно сформулювати систему заходів зі здійсненням управління ними. Розповсюдженими методами аналізу стану інформаційної безпеки є методи дослідження причинних зв’язків. За допомогою цих методів виявляються причинні зв’язки між загрозами, ризиками, викликами та небезпеками; здійснюється пошук причин, які стали джерелом і спричинили актуалізацію тих чи інших чинників небезпеки, а також розробляються заходи щодо їх нейтралізації та протидії.

«Серед даних методів причинних зв’язків можна виділити такі: метод схожості, метод відмінності, метод сполучення схожості та відмінності, метод змін, що супроводжують, метод залишків. Вибір методів аналізу стану інформаційної безпеки залежить від конкретного рівня і сфери організації захисту та протидії. У залежності від загрози стає можливим завдання щодо диференціації як різних рівнів загроз, так і різних рівнів протидії» [1].

Відносно сфери інформаційної безпеки, то у ній, зазвичай, виділяють такі рівні захисту:

- фізичний (на фізичному рівні здійснюється організація і фізичний захист інформаційних ресурсів, інформаційних технологій, що використовуються в управлінських технологіях);

- програмно-технічний (на програмно-технічному рівні здійснюється ідентифікація і перевірка відповідності користувачів, управління доступом, протоколювання і аудит, криптографія, екранування, забезпечення обмеженого доступу);

- управлінський (на даному рівні здійснюється управління, координація і контроль організаційних, технологічних і технічних заходів на всіх рівнях з боку єдиної системи забезпечення інформаційної безпеки);

- технологічний (на технологічному рівні здійснюється реалізація політики інформаційної безпеки за рахунок застосування комплексу сучасних автоматизованих інформаційних технологій);

- рівень користувача (на рівні користувача реалізація політики інформаційної безпеки спрямована на зменшення рефлексивного впливу на об'єкти інформаційної безпеки, унеможливлення інформаційного впливу з боку соціального середовища);

- мережевий (на мережевому рівні дана політика реалізується у форматі координації дій компонентів системи управління, які пов'язані між собою однією метою);

- процедурний (на процедурному рівні здійснюються заходи, що реалізовуються людьми. Серед них можна виділити наступні групи процедурних заходів: управління персоналом, фізичний захист, підтримання працездатності, реагування на порушення режиму безпеки, планування реанімаційних робіт).

Загальні методи забезпечення інформаційної безпеки активно використовуються на будь-якому етапі управління загрозами. До таких етапів належать: прийняття рішення з визначення типу та змісту інформаційної загрози й складу суб’єктів, які ведуть протидію; ухвалення загальної стратегії та алгоритму дій адекватного сприйняття загрози; виділення необхідних

ресурсів, достатніх для реалізації протидії інформаційним загрозам і збереження сталого розвитку інформаційних ресурсів в системах управління телекомунікаційних мереж; трансформації результатів оцінки ризиків у відповідну стратегію інформаційної безпеки [1].

«Вельми важливим є застосування аналітичних методів пізнання і дослідження стану професійної свідомості у сфері інформаційної безпеки. Наприклад, усвідомлення важливості забезпечення інформаційної безпеки на рівні носія інформації, структурного підрозділу і державного органу в цілому заважає розповсюджена думка про те, що захист інформації та криптографія одне й те ж саме. Водночас таке розуміння є наслідком використання застарілих підходів до інформаційної безпеки, коли поняття інформаційної безпеки передбачало лише захист інформації шляхом її шифрування» [7-8].

У наш часа важливою умовою забезпечення інформаційної безпеки є не стільки секретність, конфіденційність інформації, скільки її доступність, цілісність, захист від загроз. Отже, система має відповідно реагувати та гарантувати ефективну діяльність у цьому напрямі. Іншим завданням захисту є забезпечення незмінності інформації під час її зберігання або передавання, тобто забезпечення її цілісності [1].

«Таким чином, конфіденційність інформації, яка забезпечується за допомогою криптографічних методів не є головною вимогою при проєктуванні систем захисту інформації державних органів. Виконання процедур криптокодування і декодування може уповільнити передачу даних та зменшити доступ до них, через те, що співробітник буде позбавлений можливості своєчасного та швидкого доступу до цих даних та інформації, через функціонування механізму захисту. Саме тому, забезпечення конфіденційності інформації має відповідати можливості доступу до неї» [1].

Можна перераховувати інші методи захисту інформації, водночас, нині ототожнення забезпечення інформаційної безпеки із забезпеченням безпеки

1.2 Сучасний стан інформаційної безпеки в Україні

Інформація, яка є важливою для особи, суспільства та держави втрата якої може нанести шкоду особі, суспільству або національним інтересам держави в економічній, політичній, військової сферах, повинна захищатися від несанкціонованого ознайомлення спотворення, знищення та блокування, тобто є об'єктом захисту. Захист певної інформації є обов'язковим і про це свідчать відповідні закони України.

Інформація [information] відомості про об'єкти та явища навколишнього середовища, їхні параметри, властивості й стани, які розкривають поняття невизначеності та неповноту наших знань. У широкому розумінні інформація - це загальнонаукове поняття, що включає в себе обмін відомостями між людьми, обмін сигналами між живою й неживою природою, людьми та пристроями.

Згідно з законом України «Про інформацію» за порядком доступу інформація поділяється на відкриту інформацію та закриту з обмеженим доступом. До інформації з обмеженим доступом, за законом України, належить конфіденційна, службова та таємна інформація. Загалом, в Україні налічується близько 20 видів інформації з обмеженим доступом (адвокатська, банківська, лікарська таємниці, таємниця сповіді).

Будь-яка інформація є відкритою крім тієї що віднесена законом до інформаційї з обмеженим доступом.

Порядок віднесення інформації до таємної або службової , а також порядок доступу до неї визначається законами України.

Таємна інформація – містить державну, професійну, банківську таємницю, таємницю слідства, та іншу передбачену законом таємницю.

Конфіденційна інформація – інформація доступ до якої обмежено фізичною або юридичною особою, крім суб’єктів владних повноважень, та яка може поширюватись у визначеному ним порядку за їхніми бажанням до передбачених ними умов.

Інформаційна безпека - стан захищеності життєво важливих інтересів людини і громадянина, суспільства і держави, при якому запобігається завдання шкоди через неповноту, несвоєчасність і недостовірність поширюваної інформації, порушення цілісності та доступності інформації, несанкціонований обіг інформації з обмеженим доступом, а також через негативний інформаційно-психологічний вплив. Інформаційна безпека забезпечується діяльністю, спрямованою на запобігання, своєчасне виявлення, припинення чи нейтралізацію реальних потенційних загроз інформаційній безпеці мережі. Зокрема діяльність із запобігання порушення цілісності та доступності інформації і несанкціонованого обігу інформації з доступом складає захист інформації.

Безпека інформації – стан інформації, інформаційних ресурсів та інформаційних систем, при якому з потрібною імовірністю забезпечується захист інформації від витоку, спотворення, блокування, втрати, несанкціонованого копіювання.

Для захисту інформації в Україні створюються системи захисту інформації. Для забезпечення роботи з матеріальними носіями секретної та службової інформації і їх зберігання створюються системи охорони. Системи захисту інформації будуються за таким узагальненими етапами:

- визначення загрози для інформації та її аналіз;
- розробка політики безпеки та плану для інформації;
- розробка технічного завдання на створення системи захисту інформації;
- розробка проекту системи захисту інформації;
- упровадження системи захисту інформації;
- оцінювання ступеня захищенності інформації;
- введення системи захисту інформації в експлуатацію.

«В інформаційній сфері України вирізняються такі життєво важливі інтереси:

1) Особи:

- захищеність від негативного інформаційного впливу (в тому числі – в кіберпросторі);

- забезпечення конституційних прав і свобод людини і громадянина на збирання, зберігання, використання та поширення інформації;

- недопущення несанкціонованого втручання у зміст, процеси обробки, передачі та використання персональних даних;

2) Держави:

- забезпечення безпечного функціонування національної інформаційної інфраструктури, захист інформаційного простору України та об'єктів критичної інфраструктури держави від протиправного втручання в їх діяльність;

- захист державних інформаційних ресурсів, інформаційних ресурсів громадян і юридичних осіб, доступних за допомогою інформаційних технологій, від зовнішніх і внутрішніх загроз;

- використання для обробки державних інформаційних ресурсів апаратного та програмного забезпечення вітчизняного виробництва.» [12]

В державному кодексі України (Ст. 7) описані реальні та потенційні загрози інформаційній безпеці України.

«На сучасному етапі основними реальними та потенційними загрозами інформаційній безпеці України є:

1) у зовнішньополітичній сфері:

- поширення у світовому інформаційному просторі викривленої, недостовірної та упередженої інформації, що завдає шкоди національним інтересам України, та створює негативний імідж України, як ненадійного партнера для міжнародних відносин;

- низький рівень інтегрованості України у світовий інформаційний простір;

- прояви кіберзлочинності та кібертероризму, що загрожують сталому та безпечному функціонуванню національних інформаційно-телекомунікаційних систем;

- зовнішні деструктивні інформаційні впливи на суспільну свідомість через засоби масової інформації, а також мережу Інтернет;
- використання інформаційного простору для втручання у внутрішні справи України;

2) у сфері державної безпеки:

- ведення спеціальними службами іноземних держав розвідувально-підривної діяльності у національному сегменті кіберпростору;
- спроби втручання у внутрішні справи держави з використанням соціальних мереж,
- несанкціонований доступ та кібератаки на державні інформаційні ресурси та інформаційно-телекомунікаційні системи;
- деструктивні інформаційні впливи, спрямовані на підрив конституційного ладу, суверенітету, територіальної цілісності і недоторканності кордонів України;
- використання засобів масової інформації, а також мережі Інтернет для пропаганди сепаратизму за етнічною, мовною, релігійною та іншими ознаками;
- розголошення та виток інформації з обмеженим доступом;
- збільшення кількості злочинів із використанням сучасних інформаційно-комунікаційних технологій;
- експансія інформаційних технологій іноземних суб'єктів від належного контролю з боку держави, що послаблює інформаційну безпеку України;
- нав'язування іноземними компаніями умов функціонування національних інформаційних та телекомунікаційних мереж та систем, у тому числі на об'єктах критичної інфраструктури, що може призвести до втрати інформаційного суверенітету держави;
- недостатній рівень захищеності державних інформаційних ресурсів;

- розв’язування інформаційного протиборства (розповсюдження комп’ютерних «вірусів», встановлення програмних і апаратних закладних пристроїв, впровадження радіоелектронних приладів перехоплення інформації в технічних засобах і приміщеннях, перехоплення і дешифрування інформації, нав’язування фальшивої інформації, радіоелектронний вплив на парольно-ключові системи, радіоелектронне придушення ліній зв’язку і систем керування тощо);
- несанкціонований доступ до національних інформаційних і телекомунікаційних мереж та систем, що може порушити діяльність військових формувань, органів військового управління, Збройних Сил України в цілому, або втручання в автоматизовані системи керування зброєю.»[11]

1.3 Висновок з розділу 1

Вданному розділі були наведенні визначення таких поннять як інформація та інформаційна безпека. Також перераховано методи захисту інформації та приведенно варіанти використання медотів захисту інформації в залежності від важливості та конфіденційності даних. Було розглянуто сучасний стан інформаційної безпеки України, також наведено ряд загроз інформаційної безпеки держави та методи боротьби з ними.

2 ПРИНЦИПИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

2.1 Інформаційна безпека

Інформаційна безпека передбачає забезпечення захисту інформації та інфраструктури, що здійснює її підтримку, від будь-якого випадкового або ж зловмисного втручання, в результаті якого інформація може бути втрачена, нанесені збитки її безпосереднім власникам та інфраструктурі, що підтримує її зберігання й існування. Інформаційна безпека виконує завдання, пов’язані з прогнозуванням і запобіганням можливим подібним діям, а також зводить до мінімуму можливі збитки.

Стан інформаційної безпеки підприємства являє собою уміння і здатність підприємства протистояти будь-яким спробам завдати шкоди його законним інтересам [6].

Задачами системи інформаційної безпеки є:

− віднесення інформації до категорії обмеженого доступу;

Інформація з обмеженим доступом інформація, доступ до якої має лише обмежене коло осіб і оприлюднення якої заборонено розпорядником інформації відповідно до закону. Обмеження доступу до інформації здійснюється в інтересах національної безпеки або охорони законних прав фізичних та юридичних осіб. Обмежується доступ до інформації, а не до документу. Відповідно, якщо в одному документі міститься відкрита і закрита інформація, перша може бути надана на ознайомлення зацікавленій особі у вигляді окремого документу.

− протидія витоку такої інформації;

− прогнозування, своєчасне виявлення й усунення загроз інформаційній безпеці підприємства; причин і умов, що сприяють нанесенню фінансового, матеріального і морального збитку, порушенню нормального функціонування і розвитку;

− створення механізму й умов оперативного реагування на загрози інформаційній безпеці;

− ефективне припинення посягань на інформаційні ресурси підприємства на основі правових, організаційних і інженерно-технічних мір і засобів забезпечення безпеки [6].

Об’єктами безпеки є:

− інформація про персонал (керівництво, співробітники);

− інформація щодо технологій, які використовуються;

− інформація про клієнтах;

− інформація про проектах;

− інформаційні ресурси (інформація з обмеженим доступом, що складає комерційну таємницю, інша конфіденційна інформація, надана у вигляді документів і масивів незалежно від форми і виду їхнього представлення).

2.1 Структура інформаційно-телекомунікаційної системи типового підприємства

ІТС підприємства що забезпечує її діяльність та виконання всіх бізнес процесів та задач можна представити у вигляді ієрархії наступних основних рівнів:

− фізичного (лінії зв'язку, апаратні засоби та ін.);

− мережевого устаткування (мережеві апаратні засоби: маршрутизатори, комутатори, концентратори та ін.);

− мережевих додаткових програм і сервісів;

− операційних систем ;

− систем управління базами даних.

Основні функціональні елементі ІТС є наступні елементі ІС:

− робочі станції;

− сервери (файлів, баз даних, служб друку і т. п.);

− мережеві пристрої (маршрутизатори, комутатори, шлюзи і т. п.);

− засоби зв'язку і передачі даних;

− засоби захисту інформації;

− канали і лінії зв'язку.

Основу інформаційної системи складає база даних первинних документів, також до неї входять сервери обробки та зберігання даних із серверами додатків які реалізують таки компоненти ІТС як системи електронної пошти, системи керування та ведення проектів, системи контролю версій, бази знань [7].

Загальна схема ІТС типового підприємства зображена на рисунку 2.1

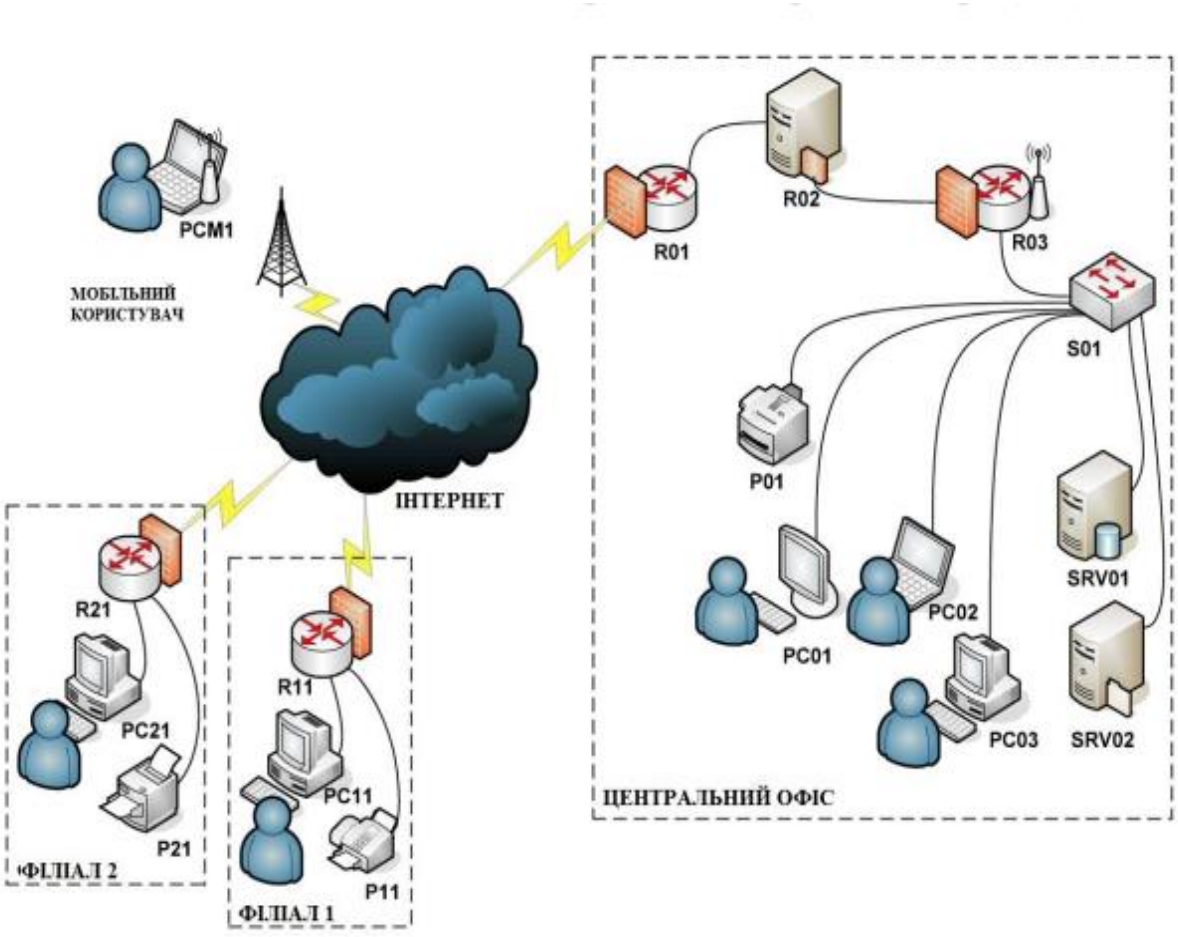

Рисунок 2.1 Загальна схема ІТС типового підприємства

2.2 Поняття загрози інформаційній безпеки підприємства

Хакерські атаки розглядаються на міжнародному рівні як частина єдиної глобальної загрози, пов'язаної з перетворенням сучасного суспільства у, так зване, «цифрове суспільство». Від зовнішніх нападів ворогів не позбавлені навіть невеликі компанії, особливо якщо вони є постачальниками або підрядниками великих корпорацій і оперують у своїй діяльності даними, здатними зацікавити зловмисників. Але й інтернет-магазини або невеликі постачальники інтернет-послуг не позбавлені DDoS-атак, здатних повністю заблокувати канали зв'язку і зробити сервіс недоступним для клієнтів.

Серед актуальних зовнішніх загроз інформаційної безпеки:

- крадіжка конфіденційної інформації шляхом злому інформаційної системи або підключення її до погано захищених каналів зв'язку. Від витоків інформації найкращим способом захищають DLP-системи, але не всі підприємства малого і середнього бізнесу мають можливість використовувати їх ресурси в повному обсязі;
- крадіжка персональних даних за допомогою власних засобів ідентифікації та передача їх посередникам на чорному ринку інформації. Цей тип загроз найбільш характерний для банків і організацій сфери послуг, що обробляють великий обсяг інформації про клієнтів;
- крадіжка інсайдерами комерційної таємниці за запитами конкурентів, найчастіше крадуть бази даних клієнтів організації;
- DDoS-атаки, спрямовані на обвалення каналів комунікації. Вони роблять сайт підприємства недоступним, що виявляється критичним для організації, що продає товари або надає послуги в Інтернеті;
- вірусні зараження. Останнім часом найбільш небезпечні віруси-шифрувальники, що роблять інформацію в системі недоступною і розблокують її за викуп. Іноді, щоб виключити можливість відстеження, хакери вимагають виплатити їм винагороду в криптовалюті;

- дефейс сайту. При цьому типі хакерської атаки перша сторінка ресурсу замінюється іншим контентом, іноді містить образливі тексти;
- фішинг. Цей спосіб скоєння комп'ютерних злочинів заснований на тому, що зловмисник направляє лист з адреси, ідентичної звичайній для кореспондента, спонукаючи зайти на свою сторінку і ввести пароль і інші конфіденційні дані, в результаті чого вони їх викрадають;
- спам, який блокує вхідні канали зв'язку і заважає відстежувати важливу кореспонденцію;
- інструменти соціальної інженерії, які спонукають співробітників компанії переводити ресурси на користь досвідченого шахрая;
- втрата даних через апаратних збоїв, несправності техніки, аварій, стихійних лих.

Загальний список загроз залишається незмінним, а технічні засоби їх реалізації удосконалюються постійно. Уразливості в штатних компонентах інформаційних систем (ОС, протоколах зв'язку) не завжди ліквідуються швидко. Так, проблеми Windows XP були усунені шляхом випуску оновлень тільки через два роки після їх фіксації. Хакери не втрачають часу, оперативно реагуючи на всі оновлення, постійно тестуючи ступінь безпеки інформаційних систем підприємства за допомогою засобів моніторингу. Особливістю сучасної ситуації на ринку комп'ютерної безпеки стало те, що машинні технології удосконалилися до того рівня, що користування ними стало доступним навіть школяреві. Заплативши невелику суму, іноді не перевищує 10 доларів, за підписку на сервіс тестування уразливості, можна організувати DDoS-атаку на будь-який сайт, розміщений на невеликому сервері з не дуже продуктивним каналом зв'язку, і в лічені хвилини позбавити клієнтів доступу до нього. Як абоненти все частіше використовуються об'єкти Інтернету речей: холодильники, кавоварки та IP-камери. Вони активно включаються в інформаційні атаки, так як виробники, що керують розробкою програмного забезпечення даних пристроїв, з метою

економії коштів, не вбудували в них механізму захисту від перехоплення управління.

Але не менш небезпечними є загрози інформаційній безпеці, які виходять від співробітників компанії, зацікавлених не в крадіжці, а в маніпуляції інформацією. Окремим ризиком стає таке порушення цілісності інформації в базах даних, що полегшує розкрадання матеріальних ресурсів організації. Прикладом може служити зміна температури зберігання палива в сторону підвищення, при якому його обсяг в цистернах збільшується і невелику відкачування датчики безпеки не помітять. Для такої зміни потрібно мати несанкціонований доступ до каналів зв'язку з пристроями, які керують виставленням температури на складі.

2.3 Джерела загроз

Джерела загроз інформаційної безпеки розуміються як вихідні підстави (причини) небезпечного впливу на життєво важливі інтереси особистості, суспільства і держави в інформаційній сфері.

Загроза – будь-які обставини або події, що можуть бути причиною порушення політики безпеки інформації і/або нанесення збитків ІС.

Загрози та їх джерела (в т.ч. зловмисники), методи і засоби захисту і підходи до оцінки ефективності можна розрізнити відповідно до рівню інформаційно-телекомунікаційна система є різними. Тому для ефективного функціонування інформаційно-телекомунікаційна систем та ведення інформаційної безпеки, необхідно розподілити інформацію за рівнями інформаційної інфраструктури.

«Рівні інформаційної інфраструктури:

− операційних систем;

− мережевих додаткових програм і сервісів;

− систем управління базами даних;

− фізичний (лінії зв'язку, апаратні засоби та ін.);

− мережевого устаткування (мережеві апаратні засоби: маршрутизатори, комутатори, концентратори та ін.);

− бізнес-процесів організації.» [10]

«Джерела загроз на фізичного, мережевого та рівня мережевих додаткових програм:

− зовнішні джерела загроз: особи, що поширюють віруси і інші шкідливі програми, хакери і інші особи, що здійснюють НСД;

− внутрішні джерела загроз: особи, що реалізовують загрози в рамках своїх повноважень і за їх межами (персонал, що має права доступу до апаратного устаткування, зокрема мережевому, адміністратори мережевих додаткових програм і тому подібне);

− комбіновані джерела загроз: зовнішні і внутрішні, такі, що діють спільно і/або погоджено» [10]

Джерела загроз на рівнях операційних систем, систем управління базами даних, технологічних процесів:

− внутрішні, такі, що реалізовують загрози в рамках своїх повноважень і за їх межами (адміністратори ОС, адміністратори СУБД, адміністратори ІБ і так далі);

− комбіновані джерела загроз: зовнішні і внутрішні, такі, що діють в змові.

Джерела загроз на рівні бізнес-процесів:

− внутрішні джерела, що реалізовують загрози в рамках своїх повноважень і за їх межами (авторизовані користувачі і оператори АБС, представники менеджменту організації і ін.);

− комбіновані джерела загроз: зовнішні (наприклад, конкуренти) і внутрішні, такі, що діють в змові.

2.4 Класифікація загроз інформаційним ресурсам підприємства

Основні загрози інформаційній безпеці підприємства:

- крадіжка інформації або витік даних (викрадення або копіювання інформації, наприклад з програми 1С, може проходити таємно та залишитися непоміченим);

- хакерські атаки (найчастіше використовують вразливості в програмному забезпеченні, тому слід користуватися ліцензованими програмами) це комплекс дій, спрямованих на пошук вразливостей в цифрових системах, наприклад на комп'ютерах, смартфонах, планшетних пристроях або навіть цілих комп'ютерних мережах. При цьому слід зазначити, що хакери не завжди займаються шкідливою діяльністю, однак сьогодні термін «хакерство» зазвичай вживається в контексті протиправних дій, а хакерами називають кіберзлочинців, які прагнуть отримати фінансову вигоду, висловити протест, зібрати певну інформацію (тобто займаються кібершпіонажем) або просто хочуть розважитися;

- халатність співробітників (недбалість і недобросовісність стосовно своїх посадових обов’язків);

- шкідливі програми (віруси, хробаки, троянські програми, програми-шпигуни, небезпечні програми та інші програми, що здатні завдати шкоди комп’ютерній безпеці) Шкідливе ПО навмисне створюється ворожим, настирливим і агресивним. Воно прагне проникнути в систему, завдати шкоди, частково перехоплення контроль над деякими діями або зовсім вивести з ладу комп'ютери, комп'ютерні системи, мережі, Планшетні та мобільні пристрої. Як і людський вірус грипу, воно заважає нормальній роботі. Мета шкідливого ПО отримання незаконного прибутку за Ваш рахунок. Попри те що шкідливе ПО не може пошкодити апаратне забезпечення системи або мережеве обладнання, воно може викрасти, Зашифровані або видалити Ваші дані, змінити функції комп'ютера або перехоплення контроль над ними. Крім того, воно може без Вашого відома Слідкуйте за активністю комп'ютера;

- СПАМ (анонімна, масова поштова розсилка з текстом небажаного характеру) це масова розсилка реклами або іншої

кореспонденції людям, які зовсім не мали бажання її отримувати. У деяких випадках, звичайно, спам може бути і корисний. Все залежить від тієї інформації, яка розсилається людям, але це буває зрідка. Найчастіше в цій розсилці вказана тільки непотрібна інформація, яка може навіть нашкодити вашому комп'ютеру. Наприклад, вам прийшов на пошту лист з посиланням на сайт, на якому є багато вірусів. В результаті ви отримуєте цілий букет "корисної" інформації:

- програмно-апаратні збої та відмови в роботі автоматизованих систем, котрі зможе усунути лише фахівець інформаційної безпеки;
- фінансове шахрайство (загрози атак із різними цілями: отримання фінансової вигоди або зривів комерційних операцій);
- крадіжка обладнання (викликає найбільший страх зі сторони керівництва, оскільки крадіжка комп’ютерів означає втрату продуктивності фірми).

Найбільш небезпечними загрозами підприємства є шкідливі програми та крадіжка інформації.

В цілому, будь-яка успішна компанія може стати жертвою атаки на конфіденційну й важливу інформацію. Тому до питання комп’ютерної безпеки потрібно відноситися відповідально. При управлінні підприємством потрібно звертати увагу на ключові елементи IT-безпеки, а саме: проводити спеціалізовані тренінги для персоналу, забезпечити захист від шкідливих програм і контенту. Також не слід забувати за допомогою IT аудиту та стежити за ситуацією в сфері інформаційних технологій підприємства.

2.5 Класифікація DLP-систем

Все DLP-системи можна розділити за рядом ознак на кілька основних класів. За здатністю блокування інформації, впізнаною як конфіденційна, виділяють системи з активним і пасивним контролем дій користувача.

Перші вміють блокувати передану інформацію, другі, відповідно, такою здатністю не володіють. Перші системи набагато краще борються з випадковими витоками даних, але при цьому здатні допустити випадкову зупинку бізнес-процесів організації, другі ж безпечні для бізнес-процесів, але підходять тільки для боротьби з систематичними витоками.

Ще одна класифікація DLP-систем проводиться за їх мережевою архітектурою. Шлюзові DLP працюють на проміжних серверах, в той час як хостові використовують агенти, що працюють безпосередньо на робочих станціях співробітників. Сьогодні найбільш поширеним варіантом є спільне використання шлюзових і хостових компонентів.

У даний час основними гравцями світового ринку DLP-систем є компанії, які широко відомі іншими своїми продуктами для забезпечення інформаційної безпеки в організаціях. Це, перш за все, Symantec, McAffee, TrendMicro, WebSense. Загальний обсяг світового ринку DLP-рішень оцінюється в 400 млн доларів, що зовсім небагато в порівнянні з тим же ринком антивірусів. Проте, ринок DLP демонструє бурхливе зростання: ще в 2009 році він оцінювався трохи більше 200 млн.

2.6 Методи аналізу потоків данихдля DLP-систем

Завдання аналізу потоку даних з метою виявлення конфіденційної інформації можна сміливо назвати нетривіальною. Оскільки пошук потрібних даних ускладнений безліччю факторів, що вимагають обліку. Тому, на сьогоднішній день розроблено декілька технологій для детектування спроб передачі конфіденційних даних. Кожна з них відрізняється від інших своїм принципом роботи.

Умовно всі способи виявлення витоків можна розділити на дві групи. До першої належать ті технології, які засновані на аналізі безпосередньо самих текстів переданих повідомлень або документів (морфологічний і статистичний аналізи, шаблони). За аналогією з антивірусним захистом їх

можна назвати проактивними. Другу групу складають реактивні способи (цифрові відбитки і мітки). Вони визначають витоку за властивостями документів або наявності в них спеціальних міток.

Морфологічний аналіз є одним з найпоширеніших тематичних способів виявлення витоків конфіденційної інформації. Суть цього методу полягає в пошуку в переданому тексті певних слів і або словосполучень.

Головною перевагою даного методу є його універсальність. З одного боку, морфологічний аналіз може використовуватися для контролю будь-яких каналів зв'язку, починаючи з файлів, що копіюються на знімні накопичувачі, і закінчуючи повідомленнями в ICQ, Skype, соціальних мережах, а з іншого - з його допомогою можуть аналізуватися будь-які тексти і відслідковуватися будь-яка інформація. При цьому конфіденційні документи не потребують будь-якої попередньої обробки. А захист починає діяти відразу після включення правил обробки і поширюється на всі задані канали зв'язку.

Основним недоліком морфологічного аналізу є відносно низька ефективність визначення конфіденційної інформації. Причому залежить вона як від використовуваних в системі захисту алгоритмів, так і від якості семантичного ядра, що застосовується для опису даних, що захищаються.

Принцип роботи статистичних методів полягає в імовірнісному аналізі тексту, який дозволяє припустити його конфіденційність або відкритість. Для їх роботи , зазвичай, потрібне попереднє навчання алгоритму. В ході нього обчислюється ймовірність знаходження тих чи інших слів, а також словосполучень в конфіденційних документах.

Перевагою статистичного аналізу є його універсальність. При цьому варто відзначити, що дана технологія працює в штатному режимі тільки в рамках підтримки постійного навчання алгоритму. Так, наприклад, якщо в процесі навчання системі було запропоновано недостатня кількість договорів, то вона не зможе визначати факт їх передачі. Тобто, якість роботи

статистичного аналізу залежить від коректності його налаштування. При цьому необхідно враховувати імовірнісний характер даної технології.

Суть методу така: адміністратор безпеки визначає строковий шаблон конфіденційних даних: кількість символів і їх тип (буква або цифра). Після цього система починає шукати в аналізованих текстах поєднання, що задовольняють його, і застосовувати до знайдених файлів або повідомленнями зазначених в правилах дії.

Головною перевагою шаблонів є висока ефективність виявлення передачі конфіденційної інформації. Стосовно до інцидентів випадкових витоків вона прагне до 100%. Випадки з навмисними пересилками - складніше. Знаючи про можливості використовуваної DLP-системи, зловмисник може протидіяти їй, зокрема, розділяючи символи різними символами. Тому використовуються методи захисту конфіденційної інформації повинні триматися в секреті.

До недоліків шаблонів відноситься, в першу чергу, обмежена сфера їх застосування. Вони можуть використовуватися тільки для стандартизованої інформації, наприклад, для захисту персональних даних. Ще одним мінусом даного методу є відносно висока частота помилкових спрацьовувань. Наприклад, номер паспорта складається з шести цифр. Але, якщо поставити такий шаблон, то він буде спрацьовувати кожного разу, коли зустрінеться 6 цифр поспіль. А це може бути номер договору, що відсилається клієнту, сума і т.п.

Під цифровим відбитком в даному випадку розуміється цілий набір характерних елементів документа, за яким його можна з високою вірогідністю визначити в майбутньому. Сучасні DLP-рішення здатні детектувати не тільки цілі файли, але і їх фрагменти. При цьому можна навіть розрахувати ступінь відповідності. Такі рішення дозволяють створювати диференційовані правила, в яких описані різні дії для різних відсотків збігу.

Важливою особливістю цифрових відбитків є те, що вони можуть використовуватися не тільки для текстових, але і для табличних документів,

а також для зображень. Це відкриває широке поле для застосування даної технології.

Принцип даного методу наступний: на вибрані документи накладаються спеціальні мітки, які видно тільки клієнтським модулям використовуваного DLP-рішення. Залежно від їх наявності система дозволяє або забороняє ті чи інші дії з файлами. Це дозволяє не тільки запобігти витоку конфіденційних документів, а й обмежити роботу з ними користувачам, що є безперечною перевагою даної технології.

До недоліків даної технології відноситься, в першу чергу, обмеженість сфери її застосування. Захистити з її допомогою можна тільки текстові документи, причому вже існуючі. На новостворювані документи це не поширюється. Частково цей недолік нівелюється способами автоматичного створення міток, наприклад, на основі набору ключових слів. Однак даний аспект зводить технологію цифрових міток до технології морфологічного аналізу, тобто, по суті, до дублювання технологій.

Іншим недоліком технології цифрових міток є легкість її обходу. Досить вручну набрати текст документа в листі (НЕ скопіювати через буфер обміну, а саме набрати), і даний спосіб буде безсилий. Тому він гарний тільки в поєднанні з іншими методами захисту.

Основні функції DLP-систем:

- контроль передачі інформації через Інтернет з використанням E-Mail, HTTP, HTTPS, FTP, Skype, ICQ і інших додатків і протоколів;
- контроль збереження інформації на зовнішні носії - CD, DVD, flash, мобільні телефони і т.п .;
- захист інформації від витоку шляхом контролю виведення даних на друк;
- блокування спроб пересилання / збереження конфіденційних даних, інформування адміністраторів ІБ про інциденти, створення тіньових копій, використання карантинної папки;

- пошук конфіденційної інформації на робочих станціях і файлових серверах за ключовими словами, мітках документів, атрибутам файлів і цифровим відбитками;
- запобігання витокам інформації шляхом контролю життєвого циклу і руху конфіденційних відомостей.

Основний функції DLP-систем візуалізовані на рисунку нижче (рис. 2.2)

Рисунок 2.2 - Основні функції DLP-систем

2.7 Висновок з розділу 2

В другому розділі розглядається стан інформаційної безпеки та її основні задачі. Також наведено об’єкти та структуру інформаційної безпеки. Розглядається основа безпеки інформації та основні поняття загрози безпеки данних. Наведені прикдали актуальних зовнішніх загроз та їх

джерела. Розглядались існуючи на данний час рівні інформаційної безпеки та класифікація загроз інформаційних ресурсів. Було визначено що кращим методом боротьби з інформаційними загрозами є системи DLP та наведена класифікація цих систем, також методи аналізу потоків даних та основні функції.

3 ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В СИСТЕМАХ УПРАВЛІННЯ ТКМ

3.1 Інформаційна безпека в системах управління ТКМ

Науково-технічний прогрес перетворив інформацію в продукт, який можна купити, продати, обміняти. Нерідко вартість даних в кілька разів перевищує ціну всієї технічної системи, яка зберігає та обробляє інформацію. Якість комерційної інформації забезпечує необхідний економічний ефект для компанії, тому важливо охороняти критично важливі дані від неправомірних дій. Це дозволить компанії успішно конкурувати на ринках телекомунікаційних послуг [4].

Інформаційна безпека (ІБ) - це стан інформаційної системи, при якому вона найменш сприйнятлива до втручання і нанесення збитку з боку третіх осіб. Безпека даних також має на увазі управління ризиками, які пов'язані з розголошенням інформації або впливом на апаратні і програмні модулі захисту.

Безпека інформації, яка обробляється в організації, - це комплекс дій, спрямованих на вирішення проблеми захисту інформаційного середовища в рамках компанії. При цьому інформація не повинна бути обмежена у використанні і динамічний розвиток для уповноважених осіб [4].

Захист інформаційних ресурсів повинен бути:

- постійний. Зловмисник в будь-який момент може спробувати обійти модулі захисту даних, які його цікавлять:
- цільовий. Інформація повинна захищатися в рамках певної мети, яку ставить організація або власник даних;
- плановий. Всі методи захисту повинні відповідати державним стандартам, законам і підзаконним актам, які регулюють питання захисту конфіденційних даних;
- активний. Заходи для підтримки роботи та вдосконалення системи захисту повинні проводитися регулярно;

- комплексний. Використання тільки окремих модулів захисту або технічних засобів неприпустимо. Необхідно застосовувати всі види захисту повною мірою, інакше розроблена система буде позбавлена сенсу та економічного підґрунтя;
- універсальний. Засоби захисту повинні бути обрані відповідно до існуючих в компанії каналами витоку;
- надійний. Всі прийоми захисту повинні надійно перекривати можливі шляхи до охоронюваної інформації з боку зловмисника, незалежно від форми представлення даних.

Інформація вважається захищеною, якщо дотримуються три головних властивості:

Цілісність - передбачає забезпечення достовірності та коректного відображення охоронюваних даних, незалежно від того, які системи безпеки та прийняття захисту використовуються в компанії. Обробка даних не повинна порушуватися, а користувачі системи, які працюють з захищеними файлами, не повинні стикатися з несанкціонованою модифікацією або знищенням ресурсів, збоями в роботі програмного забезпечення [4].

Конфіденційність – означає, що доступ до перегляду та редагування даних надається виключно авторизованим користувачам системи захисту.

Доступність - має на увазі, що всі авторизовані користувачі повинні мати доступ до конфіденційної інформації.

Досить порушити одне з властивостей захищеної інформації, щоб використання системи стало безглуздим.

На практиці створення системи захисту інформації здійснюється в три етапи.

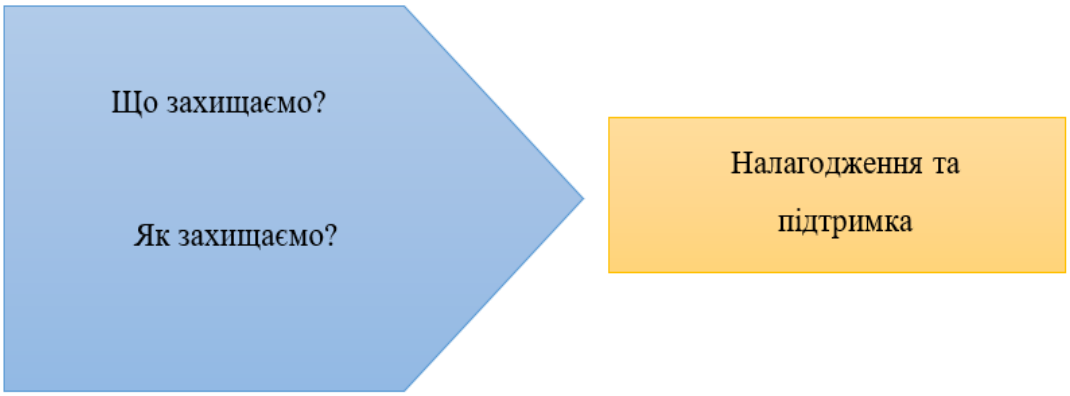

Рисунок 3.1 - Створення системи захисту

На першому етапі розробляється базова модель системи, яка буде функціонувати в компанії. Для цього необхідно проаналізувати всі види даних, які циркулюють в фірмі та які потрібно захистити від посягань з боку третіх осіб. Планом роботи на початковому етапі є чотири питання:

1. Які джерела інформації слід захистити?
2. Яка мета отримання доступу до інформації, що захищається?

Метою може бути ознайомлення, зміна, модифікація або знищення даних. Кожна дія є протиправним, якщо його виконує зловмисник. Ознайомлення не призводить до руйнування структури даних, а модифікація і знищення призводять до часткової або повної втрати інформації.

3. Що є джерелом конфіденційної інформації?

Джерела в даному випадку це люди та інформаційні ресурси: документи, флеш-носії, публікації, продукція, комп'ютерні системи, засоби забезпечення трудової діяльності.

4. Способи отримання доступу, і як захиститися від несанкціонованих спроб впливу на систему?

Розрізняють такі способи отримання доступу:

- несанкціонований доступ – незаконне використання даних;

- витік – неконтрольоване поширення інформації за межі корпоративної мережі. Витік виникає через недоліки, слабких сторін технічного каналу системи безпеки;

- розголошення – наслідок впливу людського фактора. Санкціоновані користувачі можуть розголошувати інформацію, щоб передати конкурентам, або з необережності.

Другий етап включає розробку системи захисту. Це означає реалізувати всі вибрані способи, засоби і напрямки захисту даних.

Система будується відразу по декількох напрямках захисту, на декількох рівнях, які взаємодіють один з одним для забезпечення надійного контролю інформації.

Правовий рівень забезпечує відповідність державним стандартам у сфері захисту інформації та включає авторське право, укази, патенти і посадові інструкції. Грамотно вибудувана система захисту не порушує права користувачів і норми обробки даних [4].

Організаційний рівень дозволяє створити регламент роботи користувачів з конфіденційною інформацією, підібрати кадри, організувати роботу з документацією та фізичними носіями даних [4].

Регламент роботи користувачів з конфіденційною інформацією називають правилами розмежування доступу. Правила встановлюються керівництвом компанії спільно зі службою безпеки й постачальником, який впроваджує систему безпеки. Мета – створити умови доступу до інформаційних ресурсів для кожного користувача, наприклад, право на читання, редагування, передачу конфіденційного документа. Правила розмежування доступу розробляються на організаційному рівні та впроваджуються на етапі робіт з технічної складової системи [4].

Технічний рівень умовно поділяють на фізичний, апаратний, програмний і математичний підрівні.

- Фізичний – створення перешкод навколо об'єкта, що захищається: охоронні системи, зашумлення, зміцнення архітектурних конструкцій;
- апаратний – установка технічних засобів: спеціальні комп'ютери, системи контролю співробітників, захисту серверів і корпоративних мереж;
- програмний – установка програмної оболонки системи захисту, впровадження правила розмежування доступу і тестування роботи;
- математичний – впровадження криптографічних і стенографічних методів захисту даних для безпечної передачі по корпоративній або глобальної мережі.

Третій, завершальний етап – це підтримка працездатності системи, регулярний контроль і управління ризиками. Важливо, щоб модуль захисту відрізнявся гнучкістю і дозволяв адміністратору безпеки швидко удосконалювати систему при виявленні нових потенційних загроз.

Конфіденційні дані – це інформація, доступ до якої обмежується відповідно до законів держави та нормами, які компанії встановлюються самостійно[4].

- Особисті конфіденційні дані: персональні дані громадян, право на особисте життя, листування, приховування особистості. Винятком є тільки інформація, яка поширюється в ЗМІ.
- Службові конфіденційні дані: інформація, доступ до якої може обмежити тільки держава (органи державної влади).
- Судові конфіденційні дані: таємниця слідства і судочинства.
- Комерційні конфіденційні дані: всі види інформації, яка пов'язана з комерцією (прибутком) і доступ до якої обмежується законом або підприємством (секретні розробки, технології виробництва і т.д.).
- Професійні конфіденційні дані: дані, пов'язані з діяльністю громадян, наприклад, лікарська, нотаріальна або адвокатська таємниця, розголошення якої переслідується по закону.

Загроза – це можливі або дійсні спроби заволодіти захищеними інформаційними ресурсами.

Джерелами загрози безпеці конфіденційних даних є компанії-конкуренти, зловмисники, органи управління. Мета будь-якої загрози полягає в тому, щоб вплинути на цілісність, повноту і доступність даних [4].

Загрози бувають внутрішніми або зовнішніми. Зовнішні загрози є спробами отримати доступ до даних ззовні і супроводжуються зломом серверів, мереж, акаунтів працівників і зчитуванням інформації з технічних каналів витоку (акустичне зчитування за допомогою жучків, камер, наведення на апаратні засоби, отримання віброакустичной інформації з вікон і архітектурних конструкцій) [4].

Внутрішні загрози мають на увазі неправомірні дії персоналу, робочого відділу або управління фірми. В результаті користувач системи, який працює з конфіденційною інформацією, може видати інформацію стороннім. На практиці така загроза зустрічається частіше за інших. Працівник може роками «зливати» конкурентам секретні дані. Це легко реалізується, адже дії авторизованого користувача адміністратор безпеки не кваліфікує як загрозу [4].

Спроба несанкціонованого доступу може відбуватися декількома шляхами:

- через співробітників, які можуть передавати конфіденційні дані стороннім, забирати фізичні носії або отримувати доступ до охоронюваної інформації через друковані документи;
- за допомогою програмного забезпечення зловмисники здійснюють атаки, які спрямовані на крадіжку пар «логін-пароль», перехоплення криптографічних ключів для розшифровки даних, несанкціонованого копіювання інформації;
- за допомогою апаратних компонентів автоматизованої системи, наприклад, впровадження прослуховуючих пристроїв або застосування

апаратних технологій зчитування інформації на відстані (поза контрольованою зоною).

Всі сучасні операційні системи оснащені вбудованими модулями захисту даних на програмному рівні. MAC OS, Windows, Linux, iOS відмінно справляються із завданням шифрування даних на диску і в процесі передачі на інші пристрої. Однак для створення ефективної роботи з конфіденційною інформацією важливо використовувати додаткові модулі захисту [4].

Призначені для користувача ОС не захищають дані в момент передачі по мережі, а системи захисту дозволяють контролювати інформаційні потоки, які циркулюють по корпоративної мережі, і зберігання даних на серверах [4].

Апаратно-програмний модуль захисту прийнято розділяти на групи, кожна з яких виконує функцію захисту чутливої інформації:

- Рівень ідентифікації – це комплексна система розпізнавання користувачів, яка може використовувати стандартну або багаторівневу аутентифікацію, біометрію (розпізнавання особи, сканування відбитка пальця, запис голосу та інші прийоми);
- Рівень шифрування забезпечує обмін ключами між відправником і отримувачем і шифрує / дешифрує всі дані системи.

3.2 Застосування систем DLP в системах управління ТКМ

Сьогодні ринок DLP-систем є одним з найбільш швидкозростаючих серед усіх засобів забезпечення інформаційної безпеки. Втім, вітчизняна ІБ-сфера поки не зовсім встигає за світовими тенденціями, в зв'язку з чим на ринку DLP-систем в нашій країні є свої особливості.

«Перш ніж говорити про ринок DLP-систем, необхідно визначитися з тим, що, власне кажучи, мається на увазі, коли мова йде про подібні рішення. Під DLP-системами заведено розуміти програмні продукти, що захищають організації від витоків конфіденційної інформації. Сама абревіатура DLP

розшифровується як Data Leak Prevention, тобто, запобігання витокам даних» [5].

«Подібного роду системи створюють захищений цифровий «периметр» навколо організації, аналізуючи всю виходячу, а в ряді випадків і вхідну інформацію. Контрольованої інформацією повинен бути не тільки інтернет-трафік, але і ряд інших інформаційних потоків: документи, які виносяться за межі захищається контуру безпеки на зовнішніх носіях, роздруковуються на принтері, що відправляються на мобільні носії через Bluetooth і т.д.» [5]

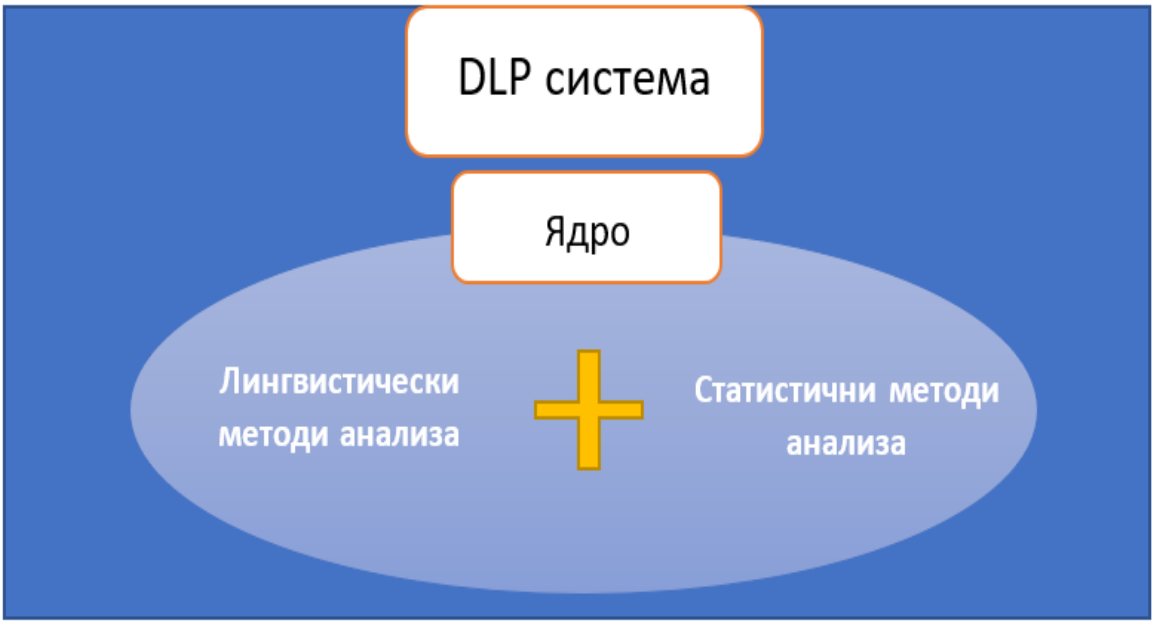

Рисунок 3.2 – Принцип роботи DLP

DLP-системи здійснюють аналіз потоків даних, які перетинають периметр захищається інформаційної системи. При виявленні в цьому потоці конфіденційної інформації спрацьовує активна компонента системи й передача повідомлення (пакета, потоку, сесії) блокується. Виявлення конфіденційної інформації в потоках даних здійснюється шляхом аналізу змісту і виявлення спеціальних ознак: грифу документа, спеціально введених міток, значень хеш-функції з певної множини та т.д.[5]

Сучасні DLP-системи володіють величезною кількістю параметрів і характеристик, які обов'язково необхідно враховувати при виборі рішення для організації захисту конфіденційної інформації від витоків. Мабуть, найважливішим з них є використовувана мережева архітектура. Згідно з цим параметром продукти розглянутого класу поділяються на дві великі групи: шлюзові (рис.3.3) і хостові (рис.3.4). У першій групі використовується єдиний сервер, на який направляється весь вихідний мережевий трафік корпоративної інформаційної системи. Цей шлюз займається його обробкою з метою виявлення можливих витоків конфіденційних даних.

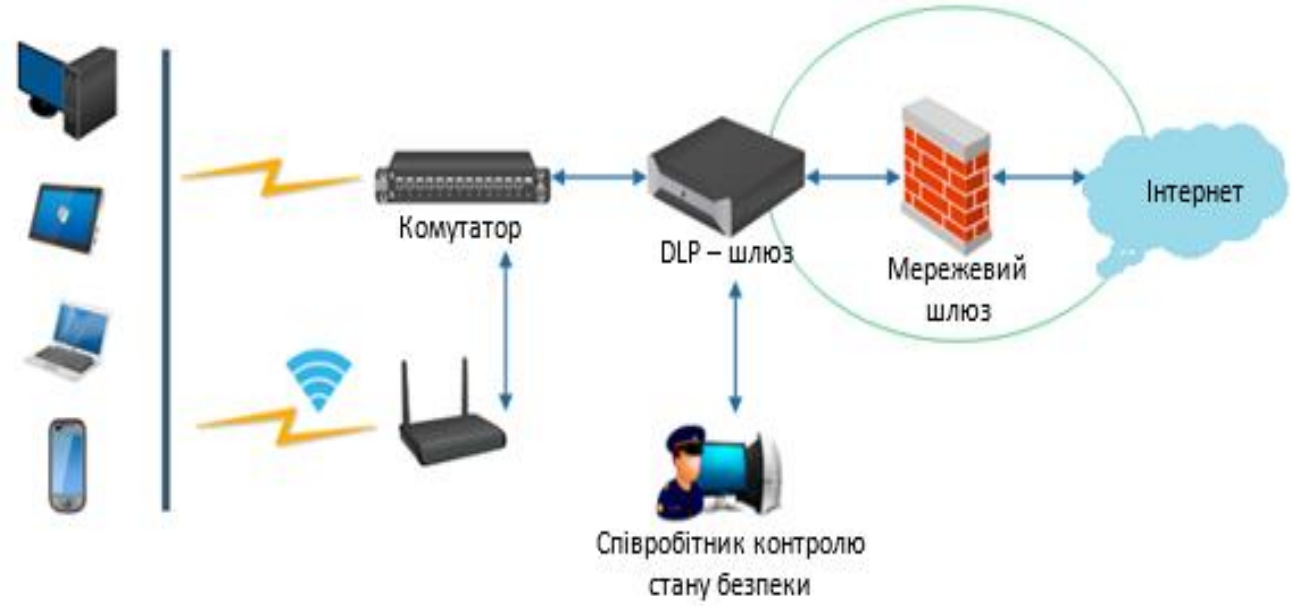

Рисунок 3.3 - Функціональна схема шлюзового DLP-рішення

Другий варіант заснований на використанні спеціальних програм – агентів, які встановлюються на кінцевих вузлах мережі – робочих станціях, серверах додатків та ін.

Рисунок 3.4 - Функціональна схема хостового DLP рішення

Останнім часом спостерігається стійка тенденція до універсалізації DLP-систем. На ринку вже не залишилося або майже не залишилося рішень, які можна було б назвати суто хостовими або шлюзовими. Навіть ті розробники, які довгий час розвивали виключно якись один напрямок, додають до своїх рішень модулі другого типу.

Причини переходу до універсалізації DLP-рішень дві. Перша з них - різні сфери застосування у систем різних типів. Як було сказано вище, хостового DLP-рішення дозволяють контролювати всякі локальні, а мережеві - інтернет-канали витоку конфіденційної інформації. Відштовхуючись від того, що в переважній більшості випадків організація потребує повної захисту, то їй потрібно і те, і інше. Другою причиною універсалізації є деякі технологічні особливості і обмеження, які не дозволяють суто шлюзовим DLP-систем повністю контролювати всі необхідні інтернет-канали.

Оскільки повністю заборонити використання потенційно небезпечних каналів передачі даних не представляється можливим, то можна поставити їх під контроль. Суть контролю полягає в моніторингу всієї інформації, що передається, виявленні серед неї конфіденційної та виконання тих чи інших

операцій, заданих політикою безпеки організації. Очевидно, що основним, найбільш важливим і трудомістким завданням є аналіз даних. Саме від його якості залежить ефективність роботи всієї DLP-системи.

Оскільки DLP-система повинна перешкоджати витоку конфіденційної інформації, то вона в обов'язковому порядку має вбудовані механізми визначення ступеня конфіденційності документа, виявленого в перехопленому трафіку. Як правило, найбільш поширені два способи: шляхом аналізу спеціальних маркерів документа і шляхом аналізу вмісту документа. Зараз більш поширений другий варіант, оскільки він стійкий перед модифікаціями, внесеними в документ перед його відправкою, а також дозволяє легко розширювати число конфіденційних документів, з якими може працювати система.

Крім свого основного завдання, пов'язаного із запобіганням витоків інформації, DLP-системи також добре підходять для вирішення ряду інших завдань, пов'язаних з контролем дій персоналу.

Найбільш часто DLP-системи застосовуються для вирішення наступних неосновних для себе завдань:

- контроль використання робочого часу та робочих ресурсів співробітниками;
- моніторинг спілкування співробітників з метою виявлення «підкилимної» боротьби, яка може нашкодити організації;
- контроль правомірності дій співробітників (запобігання друку підроблених документів та ін.);
- виявлення співробітників, що розсилають резюме, для оперативного пошуку фахівців на посаду, що звільнилася.

За рахунок того, що багато організацій вважають ряд цих завдань (особливо контроль використання робочого часу) більш пріоритетними, ніж захист від витоків інформації, виник цілий ряд програм, призначених саме для цього, однак здатних в ряді випадків працювати і як засіб захисту організації від витоків . Від повноцінних DLP-систем такі програми відрізняє

відсутність розвинених засобів аналізу перехоплених даних, яка повинна проводитися фахівцем із інформаційної безпеки вручну, що зручно тільки для зовсім невеликих організацій (до десяти контрольованих співробітників).

3.3 Управління інцидентами інформаційної безпеки в системах управління ТКМ

Система захисту від витоків інформації грунтується в тому числі на виявленні, запобіганні, реєстрації та усунення наслідків інцидентів інформаційної безпеки або подій, що порушують регламентовані процедури захисту ІБ. Існує ряд методик, що визначають основні параметри управління ними. Ці методики впроваджуються на рівні міжнародних стандартів, що встановлюють критерії оцінки якості менеджменту в компанії. Події або інциденти ІБ в рамках цих регламентів виявляються і реєструються, їх наслідки усуваються, а на підставі аналізу причин їх виникнення положення і методики допрацьовуються [5].

Міжнародні регламенти, які діють в сфері сертифікації менеджменту інформаційних систем, дають своє визначення цьому явищу. Згідно з ними інцидентом інформаційної безпеки є одинична подія небажаного і непередбачуваний характер, яке здатне вплинути на бізнес-процеси компанії, скомпрометувати їх або порушити ступінь захисту інформаційної безпеки. На практиці до цього поняття відносяться різнопланові події, що відбуваються в процесі роботи з інформацією, яка існує в електронній формі або на матеріальних носіях. До них може ставитися і залишення документів на робочому столі у вільному доступі для іншого персоналу, і хакерська атака –обидва інциденти в рівній мірі можуть завдати шкоди інтересам компанії[5].

Серед основних типів подій присутні:

- порушення порядку взаємодії з Інтернет-провайдерами, хостингами, поштовими сервісами, хмарними сервісами та іншими постачальниками телекомунікаційних послуг;
- відмова обладнання з будь-яких причин, як технічного, так і програмного характеру;
- порушення роботи програмного забезпечення;
- порушення будь-яких правил обробки, зберігання, передачі інформації, як електронної, так і документів;
- неавторизований або несанкціонований доступ третіх осіб до інформаційних ресурсів;
- виявлення зовнішнього моніторингу ресурсів;
- виявлення вірусів або інших шкідливих програм;
- будь-яка компрометація системи, наприклад, потрапляння пароля від облікового запису у відкритий доступ.

Всі ці події повинні бути класифіковані, описані і внесені у внутрішні документи компанії, які регламентують порядок забезпечення інформаційної безпеки. Крім того, в регламентуючих документах необхідно встановити ієрархію подій, розділити їх на більш-менш значущі. Слід враховувати, що істотна частина інцидентів малопомітні, вони відбуваються поза периметром уваги посадових осіб. Такі події повинні бути описані окремо, а визначені заходи для їх виявлення в режимі постфактум [5].

При описі заходів реакції слід враховувати, що зміна частоти появи і загальної кількості інцидентів інформаційної безпеки є одним з показників якості роботи систем, що забезпечують ІБ, і саме по собі класифікується як істотного події. Почастішання подій може говорити про навмисні атаки на інформаційні системи компанії, тому вони повинні стати підставою для аналізу і подальшого підвищення рівня захисту [5].

Регламенти, що визначають порядок управління інцидентами інформаційної безпеки, повинні стати складовою частиною бізнес-процесів і їх регламентації. Припускаючи, що інцидентом є недозволена,

несанкціонована подія, в роботі потрібно спиратися на механізм, що розділяє події і дії на дозволені і заборонені, що визначає органи, які мають права на розробку таких норм. Крім того, регламент визначає методи і способи класифікацій подій, прямо не зазначених у документах як значимих, і механізм виявлення таких подій, їх опису та подальшого внесення в регламентуючі документи.

Наприклад, в регламенті може бути заборонено розміщення конфіденційної інформації на портативних носіях без її кодування або шифрування, при цьому не буде прямо встановлено заборону на винос таких пристроїв за межі компанії. Випадкова втрата комп'ютера в результаті злочинного посягання стане інцидентом, але він не буде прямо забороненим. Відповідно, в документах повинен бути встановлений механізм доповнення норм і правил безпеки в ситуативному порядку без зайвої бюрократії. Це дозволить оперативно реагувати на нові виклики і допрацьовувати заходи захисту своєчасно, а не зі значним запізненням [5].

Система сертифікації ISO 27001 в якості одного з елементів ІБ передбачає необхідність створення окремої процедури управління інцидентами інформаційної безпеки в рамках загальної системи стандартизації бізнес-процесів.

Незважаючи на те, що стандарти прямо рекомендують впроваджувати методики управління інцидентами інформаційної безпеки, на практиці впровадження та реалізації цих практик зустрічають безліч складнощів. Окремі процедури управління інцидентами не впроваджуються. Цей показник не говорить про те, що система менеджменту інцидентів працюють добре чи погано, це свідчить тільки про те, що існує певний пролом в системі безпеки.

Управління інцидентами інформаційної безпеки засноване на наступних діях:

- визначення. В організації відсутня методика виявлення і класифікації інцидентів, опис їх основних параметрів, тому співробітники

встають перед необхідністю або самостійно визначати критерії події, або ігнорувати його. Вхід в мережу під обліковим записом іншого співробітника, відповідно до стандартів, є інцидентом інформаційної безпеки, але він не буде зафіксований в журналі, так як співробітники вважають таку поведінку стандартним і дозволеним, особливо в умовах дефіциту кадрових ресурсів;

- оповіщення про виникнення. Навіть якщо яка-небудь подія може бути визначено згідно з прийнятими в організації методикам або особисту думку співробітника як інцидент, найчастіше в організації не розроблені стандарти і маршрути оповіщення про такі події. Навіть якщо кимось буде виявлено факт копіювання документів, що відносяться до комерційної таємниці, співробітник встане в безвихідь перед питанням, хто саме і в якій формі має бути сповіщений про цей інцидент: його керівник, служба безпеки або інша особа;

- реєстрація. Ця частина стандартів є найбільш нездійсненним для російських компаній, інциденти не ідентифікуються, відповідно, не фіксуються. Відсутня практика закладу регістрів обліку, в яких би фіксувалися значущі події, що згодом давало б матеріал для їх аналізу і прогнозу можливих атак;

- усунення причин і наслідків. Будь інцидент викликає певні сліди і наслідки, які, з одного боку, можуть заважати діяльності компанії, з іншого - служать матеріалом для проведення розслідування причин його виникнення. Відсутність регламентів усунення наслідків може привести як до накопичення помилок, так і до повного знищення доказової бази, що дозволяє виявити винуватця сталася ситуації. Будь-які термінові заходи, що вживаються для відновлення стабільності, можуть випадково або навмисно знищити сліди проникнення в базу даних;

- заходи реагування на інциденти. У ряді випадків виникнення інциденту може вимагати термінових заходів реагування, наприклад, відключення комп'ютера від мережі, припинення передачі інформації, установки контакту з провайдером. Повинні бути визначені органи і посадові

особи, відповідальні за розробку механізму реагування і його оперативну реалізацію;

- розслідування. Повноваження по розслідуванню повинні бути передані з відання IT-служби в компетенцію служб безпеки. У рамках розслідування повинні бути вивчені журнали обліку, проаналізовані дії всіх користувачів і адміністраторів, які мали доступ до систем в період виникнення надзвичайної ситуації. Розслідування повинно стати одним з основних елементів управління інцидентами. На практиці в російських компаніях від реалізації цього етапу відмовляються, обмежуючись усунення наслідків події, що сталася. При необхідності розслідування повинно проводитися із залученням оперативно-слідчих органів;

- реалізація превентивних заходів. У більшості випадків інциденти не є поодинокими, їх виникнення свідчить про те, що в системі ІБ виникла пролом і аналогічні випадки будуть повторюватися. Щоб уникнути цих ризиків необхідно за результатами розслідування підготувати протокол або акт комісії, в якому визначити, які саме заходи повинні бути застосовані для запобігання аналогічних ситуацій. Крім того, застосовуються певні заходи дисциплінарної відповідальності, передбачені Трудовим кодексом і внутрішніми регламентами;

- аналітика. Всі події, що порушують регламентовані процеси і можуть бути кваліфіковані як інциденти інформаційної безпеки, повинні стати основою для аналізу, який допоможе визначити їх характер, проявити системність і виробити рекомендації для вдосконалення системи ІБ, діючу пенсійну систему компанії.

Основні проблеми, пов'язані з порушенням процедур, обумовлені неготовністю персоналу в повній мірі сприймати, адаптувати і виконувати рекомендації. Відносно інцидентів інформаційної безпеки, складності в сприйнятті та реакції викликають моменти, пов'язані з вчиненням дій, які прямо не регламентовані інструкціями або стандартами або викликають відчуття зайвих або надлишкових.

Як будь-яка корпоративна процедура, організація управління інцидентами інформаційної безпеки повинна пройти кілька етапів: від прийняття рішення про його необхідність до впровадження та аудиту. На практиці менеджмент більшості підприємств не усвідомлює необхідності застосування цієї практики захисту інформаційного периметра, тому для виникнення ініціативи про її впровадження часто потрібно аудит систем ІБ зовнішніми консультантами, вироблення ними рекомендацій, які потім будуть реалізовані керівництвом підприємства. Таким чином, початковою точкою для реалізації процедур управління інцидентами ІБ стає рішення виконавчих органів або іноді більш високих ланок системи управління компанії, наприклад, Ради директорів [5].

Загальне рішення зазвичай приймається в руслі модернізації існуючої системи ІБ. Система управління інцидентами є її основною частиною. На рівні прийняття рішення необхідна його локалізація в загальній парадигмі цілей компанії. Оптимально, якщо функціонування системи ІБ стає однією з бізнес-цілей організації, а якість її роботи підкріплюється встановленням ключових показників ефективності для відповідальних співробітників компанії. Після визначення статусу функціонування системи необхідно перейти до розробки внутрішньої документації, яка направлена безпосередньо на пов'язані з нею відносини в компанії.

Для додання значущості методикам управління інформаційною безпекою вони повинні бути затверджені на рівні виконавчого органу (генерального директора, правління або ради директорів). З даними документа необхідно ознайомити всіх співробітників, що мають відношення до роботи з інформацією, яка існує в електронних формах або на матеріальних носіях.

3.4 Перспективи і тенденції

Головною тенденцією, як вважають експерти, є перехід від «позаплатових » систем, що складаються з компонентів від різних виробників, які вирішують кожен своє завдання, до єдиних інтегрованих програмним комплексам. Причина подібного переходу очевидна: комплексні інтегровані системи позбавляють фахівців з інформаційної безпеки від необхідності вирішувати проблеми сумісності різних компонентів системи між собою, дозволяють легко змінювати налаштування відразу для великих масивів клієнтських робочих станцій в організаціях, а також дозволяють не відчувати труднощів при перенесенні даних з одного компонента єдиної інтегрованої системи в інший. Також рух розробників до інтегрованих систем йде в силу специфіки завдань забезпечення інформаційної безпеки: адже якщо залишити без контролю хоча б один канал, по якому може статися витік інформації, не можна говорити про захищеність організації від подібного роду погроз[5].

Західні виробники DLP-систем, що прийшли на ринок країн СНД, зіткнулися з низкою проблем, пов'язаних з підтримкою національних мов. Оскільки ринок СНД вельми цікавий західним вендорам, сьогодні вони ведуть активну роботу над підтримкою російської мови, яка є основною перешкодою для їх успішного освоєння ринку.

Ще однією важливою тенденцією в сфері DLP є поступовий перехід до модульної структури, коли замовник може самостійно вибрати ті компоненти системи, які йому необхідні (наприклад, якщо на рівні операційної системи відключена підтримка зовнішніх пристроїв, то немає необхідності доплачувати за функціональність по їх контролю). Важливу роль на розвиток DLP-систем буде надавати і галузева специфіка - цілком можна очікувати появу спеціальних версій відомих систем, адаптованих спеціально для банківської сфери, для держустанов і т.д., що відповідають запитам самих організацій[5].

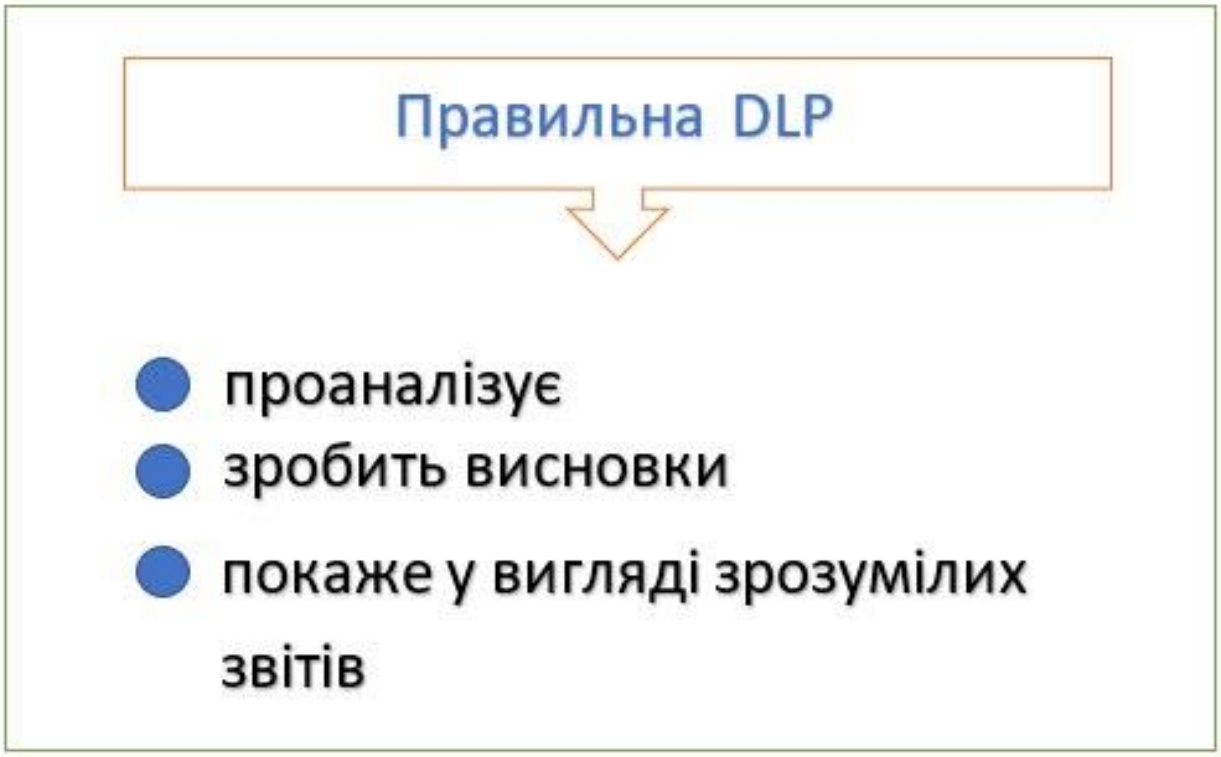

Рисунок 3.5 – Основні функції DLP-системі

Важливим фактором, що впливає на розвиток DLP-систем, є також поширення ноутбуків і нетбуків в корпоративних середовищах. Специфіка лептопів (робота поза корпоративного середовища, можливість крадіжки інформації разом з самим пристроєм і т.д.) змушує виробників DLP-систем розробляти принципово нові підходи до захисту портативних комп'ютерів. Варто зазначити, що сьогодні лише деякі вендори готові запропонувати замовнику функцію контролю ноутбуків і нетбуків своєї DLP-системою[5].

3.5 Висновок з розділу 3

В даному розділі розглядалась інформаційна безпека в системах управління ТКМ та основні поняття. Було наведено приклади яким повинен бути захист інформаційних ресурсів та розглянуто етапи створення систем захисту даних.

Наводились приклади способів доступу до інформації, описано що являти собою DLP-системи та розглянуто в яких випадках застосовуються система DLP в системах управління ТКМ. Розповідалось про принцип роботи систем DLP, наведенні функціональні схеми. Розглянуто методи управління інцидентами безпеки в системах управління ТКМ.

ВИСНОВКИ

У дипломної роботи були наведенні визначення таких поннять як інформація та інформаційна безпеки в системах управління ТКМ. Також перераховано методи захисту інформації та приведенно варіанти використання медотів захисту інформації в залежності від важливості та конфіденційності даних. Було розглянуто сучасний стан інформаційної безпеки України, також наведено різновид загроз інформаційної безпеки держави.

Було розглядається стан інформаційної безпеки та її основні задачі, також наведено об’єкти та структуру інформаційної безпеки. Розглядається основа безпеки інформації та основні поняття загрози безпеки данних. Наведені прикдали актуальних зовнішніх загроз. Розглядались існуючи на данний час рівні інформаційної безпеки та класифікація загроз інформаційних ресурсів. Було визначено що кращим методом боротьби з інформаційними загрозами є системи DLP та наведена класифікація цих систем, також методи аналізу потоків даних та основні функції. В дипломній роботі було наведино приклади способів доступу до інформації, описано що представляють з себе DLP-системи та розглянуто в яких випадках застосовуються система DLP в системах управління телекомунікаційних мереж. Розповідалось про принцип роботи систем DLP, наведенні функціональні схеми. Розглянуто методи управління інцидентами безпеки в системах управління телекомунікаційних мереж.

На підставі вище сказаного вважаю, що мету дипломної роботи виконано повною мірою.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Асанович В.Я. Информационная безопасность: анализ и прогноз информационного воздействия / В.Я. Асанович, Г.Г. Маньшин. – Мн.: Амалфея, 2006. – 204 с.
2. Кормич Б.А. Інформаційна безпека: організаційноправові основи / Б.А. Кормич. – К.: Кондор, 2003. – 384 с.
3. https://searchinform.ru/informatsionnaya-bezopasnost/
4. https://searchinform.ru/informatsionnaya-bezopasnost/dlp-sistemy/
5. http://ir.nmu.org.ua/bitstream/handle/123456789/151307/Сударикov.pdf?sequence=3&isAllowed=y
6. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 1.1–002–99.–К.. ДСТСЗІ СБ України, 1999. – 16 с
7. Пєвцов Г.В. Концептуальні підходи щодо забезпечення інформаційної безпеки у воєнній сфері / Г.В. Пєвцов, С.В. Залкін, А.О. Феклістов // Системи обробки інформації. – 2011. – Вип. 2 (92). – С. 57-59.
8. Семенченко А.І. Методологія стратегічного планування у сфері державного управління забезпеченням національної безпеки України: моногр. / А.І. Семенченко. – К.: Вид-во НАДУ, 2008. – 428 с.
9. http://www.hups.mil.gov.ua/periodicapp/article/16818/zhups_2016_2_11.pdf
10. http://www.consultant.ru/document/cons_doc_LAW_102090/5de80b568ffe66904f29481ba76842b65d3806a9/
11. https://zakon.rada.gov.ua/laws/show/964-15
12. http://search.ligazakon.ua/l_doc2.nsf/link1/T030435.html
13. ОСНОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ Заплотинський Б.А.